APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,899	06/14/2001	Chee-Hong Wong	20735-05503	8876

758   7590   03/25/2005

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER
SON, LINH L D

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/881,899	WONG ET AL.
	Examiner	Art Unit
	Linh Son	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*14 June 2001*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*1-26*</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration. .

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*1-26*</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>*09/01, 05/02*</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is responding to the application filed on June 14th, 2001.

2.   Claims 1-26 are pending.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over

smith et al, US Patent No. 6061448, hereinafter "Smith".

5.   As per claim 1, Smith teaches "A computer-implemented method for securely

transmitting an information package from a sender to an addressee via a network (Col 5

lines 38-44), the method comprising a server system performing the steps of: receiving

a delivery from the sender (Col 6 lines 45-54), the delivery comprising: the information

package encrypted with a package encryption key (Col 5 lines 38-65); and a package

decryption key encrypted with an escrow key (Col 5 lines 30-37, the user public key);

storing the delivery in escrow for the addressee; sending to the addressee a notification

of the delivery (Col 5 lines 5-15); and in response to receiving an acknowledgement

from the addressee: obtaining a new public key of the addressee (Col 5 lines 5-15);

decrypting the package decryption key; encrypting the package decryption key with the

addressee's new public key (Col 5 line 60 to Col 6 line 10); and transmitting to the

addressee the information package encrypted with the package encryption key and the

package decryption key encrypted with the addressee's new public key (Col 5 line 60 to

Col 6 line 10). However, Smith does not teach of the escrow key directly and a re-

encryption process using the new generated public key of the addressee at the server.

Nevertheless, Smith utilizes the addressee's public key as the escrow key (Col 5 lines

37-45), also teaches of having capability to regenerate new key for the session (Col 5

lines 5-15), and having a capability of encrypting at the server using the addressee's

public key (Col 5 lines 60-67). Therefore, it would have been obvious at the time of the

invention was made for one having ordinary skill in the art to modify the invention to

generate a new public key for the addressee for every new deliveries session received

at the server. The second re-encryption process will help to protect the package and to

prevent the possibility of compromised public key during the previous transmission

process to both sender and receiver.

6.   As per claims 11, and 18, Smith teaches "A system, a method and an apparatus

for securely transmitting an information package from a sender to an addressee via a

network (Col 4 lines 1-67, and Col 6 lines 65-67), the system comprising: a storage

module, comprising a computer-readable storage medium, for receiving, and storing in

escrow, a delivery from the sender (Col 6 line 40 to Col 7 line 30), said delivery

comprising: a package decryption key encrypted with an escrow key, and the
information package encrypted with a package encryption key (Col 5 line 60 to Col 6
line 10); a key registration module coupled to the notification module for, in response to
receiving an acknowledgement from the addressee, receiving a new public key of the
addressee (Col 5 lines 5-15); and for transmitting to the addressee the information
package encrypted with the package encryption key and the package decryption key
encrypted with the addressee's new public key (Col 8 line 50 to Col 10 line 46).
However, Smith does not teach of the escrow key directly and a re-encryption process
using the new generated public key of the addressee at the server. Nevertheless,
Smith utilizes the addressee's public key as the escrow key (Col 5 lines 37-45), also
teaches of having capability to regenerate new key for the session (Col 5 lines 5-15),
and having a capability of encrypting at the server using the addressee's public key (Col
5 lines 60-67). Therefore, it would have been obvious at the time of the invention was
made for one having ordinary skill in the art to modify the invention to generate a new
public key for the addressee for every new deliveries session received at the server.
The second re-encryption process will help to protect the package and to prevent the
possibility of compromised public key during the previous transmission process to both
sender and receiver.

7.   As per claims 2 and 19, Smith teaches "The method of claims 1 and 18, further
comprising the server system performing the steps of: receiving a request from the
sender for a public key of the addressee; determining whether the addressee has a

public key; and in response to not finding a public key of the addressee: transmitting the

escrow key to the sender" in (Col 5 lines 5-15).

8.   As per claims 3 and 20, Smith teaches "The method of claims 2 and 19, wherein

the step of determining whether the addressee has a public key comprises the sub-step

of: checking a public key database for a public key of the addressee" in (Col 6 lines 40-

65).

9.   As per claims 4 and 21, Smith teaches "The method of claims 1 and 18, further

comprising the server system performing the steps of: in response to the sender

searching a public key database for a public key of the addressee and not finding a

public key of the addressee: receiving a request from the sender for the escrow key;

and transmitting the escrow key to the sender" in (Col 6 lines 40-65).

10.   As per claims 5, 13-14, and 22, Smith teaches "The method of claims 1, 11, and

18, further comprising the server system performing the steps of: registering and issuing

the new public key to the addressee; and storing the addressee's new public key in a

public key database" in (Col 5 lines 1-15).

11.   As per claims 6 and 15, Smith teaches "The method of claims 1 and 11, wherein

the escrow key is one of a group comprising a symmetric key and an asymmetric key" in

(Col 4 lines 8, asymmetric key equals to public/private key).

12.   As per claims 7, 16, and 23, Smith teaches "The method of claims 1, 11, and 18

wherein the notification is one of a group comprising an e-mail notification, a desktop

notification, a voice notification, a pager notification, and a facsimile notification" in (Col

5 lines 1-15).

13.   As per claims 8 and 24, Smith teaches "The method of claims 1 and 18, further

comprising the server system performing the steps of: receiving from the sender a

digest of one from a group comprising: the information package; the information

package encrypted with the package encryption key; and the information package

encrypted with the package encryption key and the package decryption key encrypted

with the escrow key; and in response to receiving the acknowledgement from the

addressee: transmitting the digest to the addressee" in (Col 5 lines 1-30, and Col 6 lines

40-67).

14.   As per claims 9, 25, Smith teaches "The method of claims 8 and 25, wherein the

digest is encrypted by a private key of the sender" in (Col 3 lines 1-6).

15.   As per claim 12, Smith teaches "The system of claim 11 further comprising: a

directory interface coupled to the storage module for checking, in response to receiving

a request from the sender for a public key of the addressee, a public key database for

the public key of the addressee; and an escrow key manager coupled to the directory

interface for providing, in response to the directory interface failing to obtain a public key

of the addressee from the public key database, an escrow key for encrypting the

package decryption key" in (Col 5 lines 1-52, public key of the addressee is interpreted
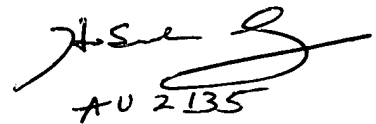
as the escrow key).

16.   As per claims 10, 17, and 26, Smith teaches "The computer-readable medium of

claims 1, 11, and 18, further comprising program code adapted to perform the step of:

authenticating the addressee prior to transmitting the information package encrypted

with the package encryption key and the package encryption key encrypted with the

addressee's new public key" in (Col 5 lines 1-53) and the rejection of claim is

incorporated.

Conclusion

17.   Any inquiry concerning this communication from the examiner should be directed

to Linh Son whose telephone number is (571)-271-3856.

18.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this

group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the

status of this application or proceeding should be directed to the group receptionist

whose telephone number is (571)-272-2100.

19.   Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval IPAIR.I system. Status information for

published applications may be obtained from either Private PMR or Public PMR. Status

information for unpublished applications is available through Private PMR only. For

more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son

Patent Examiner